IN THE SPECIFICATION

The following paragraphs will replace all prior versions in the Specification.

[0001] This application claims priority to Provisional Application Serial No. 60/334,754 ~~60xxxxxx~~, filed October 19, 2001.

[0004] Security is achieved by the use of a combination of software and hardware measures. Software employing a variety of cryptographic techniques is used to encrypt and/or authenticate the information exchanged through the network while hardware-based physical security measures guarantee that the cryptographic keys and the software using these keys remain uncorrupted, private and trustworthy. The software and cryptographic techniques used depend on the services, resources and information accessed through the network; for example, a network security device that supports Virtual Private Networking (VPN) functionality will have software that implements IPsec, Point-to-Point Tunneling Protocol (PPTP) ~~PPTP~~ or some other VPN protocol. This software will use cryptographic keys in the way specified by the VPN protocol in use to encrypt and/or authenticate all information flowing to and fro the network.

[0013] In addition to the security ROM 18 (and the write-once ROM 20 if present), the security mechanism 10 of FIG. 1 also includes at least one "persistent" memory element 24, in the form of a Complementary Metal Oxide Semiconductor ~~CMOS~~ Random Access Memory (CMOSRAM) or a Programmable Read Only Memory (PROM) for receiving data prior to or during a communications session and for retaining such data for use during a subsequent session. In FIG. 1, the memory element 24 bears the designation "Configuration Memory" because this memory element stores configuration data that enables the security mechanism 10 to facilitate a connection with different networks. Thus, the contents of the Configuration memory element 24 can change upon an application executed by the network peripheral 12 that requires new or updated configuration information. To maintain security, only the application requiring new or updated configuration information should have the ability to write data to the configuration memory element 24 and the data written to this area must be of a nature

that could compromise the security afforded to the user. In other words, security critical data (i.e., data identifying the user and the device) must be excluded. The application executed by the network peripheral device 12 that seeks to write data to the Configuration Memory Element 24 should require signing and that such signing should be verified by the information in the Security ROM 18.

[0014] In addition to the previously described memory elements, the security mechanism 10 also includes at least one volatile memory element 26 in the form of a Random Access (RAM) memory or the like. The RAM 26 holds session-specific data, including user-entered verification data, such as a password or Personal Identification Number (PIN) ~~PIN~~, as well as authentication data generated by the security mechanism 10 itself. The data held within the RAM 26 remains only for the duration of a session. At the end of each session, as well as upon a power-down condition, the bootstrap code within the Security ROM 18 (or the bootstrap code in the Write-Once ROM 20) causes the RAM 26 to erase all of its data (or at least its sensitive security data) if such data has not already been erased. In this way, the memory element 26 loses all user-entered verification data, as well as all security mechanism-generated authentication data associated with a given session upon its completion, or upon a power-down condition.

[0018] The invention describes a method for hardening a security mechanism against physical intrusion ~~attacks~~ and ~~against~~ substitution attacks. A user establishes a connection between a network peripheral device (12) and a network (14) via a security mechanism (10) ~~that provides the security functions necessary to access the resources of the network (14)~~. The security mechanism (10) includes read only memory (ROM) (22) that contains ~~the bootstrap application~~ code that initiates ~~the~~ operation of the mechanism and ~~as well as~~ performs ~~the required~~ authentication functions. A persistent memory (24) contains configuration information ~~that enables the security mechanism to configure the device to the network~~. A volatile memory (26) stores user and device identification information that remains valid only for a given session and is erased thereafter to prevent ~~so that a past successful connection won't facilitate~~ a future

security breach. A tamper-evident enclosure (32) surrounds the memory elements ~~to provide physical security~~, which if breached, becomes readily apparent to the user. The software stored in the ROM (22) must be constructed so that a future compromise of the device will not adversely affect the security of past sessions and so that ~~any~~ data that ~~will affect~~ affects the level of security provided to the user is obtained ~~from the user~~ at the beginning of each session.